ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

# Comparative Study of Different Password Managers and Insight of Bilateral Password Manager

Shubham Agarwal [1], Ikhlas Shaikh [1], Ujjawal Tripathi [1], Shubhangi Khade [2]

U.G. Student, Department of Computer Engineering, Modern Education Society's College of Engineering, Pune, Maharashtra, India. [1]

Associate Professor, Department of Computer Engineering, Modern Education Society's College of Engineering, Pune, Maharashtra, India. [2]

**ABSTRACT:** With the emergence of digital technologies a need for privacy and security arose which was mostly fulfilled by passwords. Though, these passwords are also a potential point of failure and a burden. Password managers have provided a convenient way to manage them. The goal is to provide users with a much more secured and easy management of their passwords. The proposed system is a generative password manager i.e. it generates passwords for the user instead of retrieving them from the database. It divides the password generation key in two parts, and generates the complex passwords using a secret key stored in user's client application and another key stored on the server. It also improves the password strength substantially by creating passwords itself rather than requiring the user to do so.

**KEYWORDS**: password, generative password manager, strong recovery, multiple access.

## I. INTRODUCTION

With the emergence of new digital services like e-mails, digital media, e-commerce, etc. the number of accounts a single person holds across various websites has increased substantially. An average internet user has about 18 online accounts. Despite passwords being vulnerable most websites still use password based authentication. As the number of accounts are more, the user nowadays uses easy passwords and even common passwords across different sites. This makes the user's accounts vulnerable to breaches. A single breach can compromise all the accounts. The problem of many account ids and their password to remember has also led to a situation where recovery tools are being used a lot to recover the accounts in case of loss of password. The solution to get rid of or mitigate these possible failure points is a password manager. A password manager helps the user by storing all the account ids and their password securely. The only password the user will have to remember is of the password manager i.e. the master password.

Many password managers are available in the market today but they all have their cons. They may be prone to single point of failure, be inconvenient to use, have poor recoverability, etc. This makes them vulnerable and also not reliable and usable. Use of highly secure ways to store and manage passwords is needed. On the other hand, a highly secured system is also of not much use if it is not usable. It may instead end up becoming a burden for the user. The proposed system gets rid of these issues by using various features to give the users an enhanced, secure and convenient system for the managing their account credentials.

## II. LITERATURE SURVEY

The digitalization of the world and the subsequent increase in number of online accounts a person has actually increased the impact of passwords on a user's life. Simple services like paying bills, getting directions, watching movies, chatting, etc. have all been digitized. A user can now easily be harmed financially, emotionally on the internet.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

Though, the novice internet user isn't aware of the potential dangers of the digitally connected world. To secure against attacks from hackers and safeguard his passwords, the keys to all his accounts, which control his money and his private data the user must be protected. Password remembering is a big task for the user and most users use easy and common passwords so that it can be remembered easily. Users also use same password across different accounts to ease the remembering part. The user may use comparatively hard passwords but these often get repeated or lead to the user forgetting the password. In this paper [1], a survey of 30 people has been done and results shows that different people have different techniques to remember the difficult passwords and so it provides some techniques to remember passwords which are not easy to guess. Though it can help a bit but with so many possible accounts, a user will have to remember many account ids and their related password, which is difficult. Some methods have been tried to make passwords safe. QR images are being used for authentication nowadays. In this paper [2], the user has to remember a sequence of QR images to log into the account. It works as a 2 step authentication to enhance the security. A potentially major weakness in this case would be if the QR code generation methodology is compromised. This would make each and every account free to use. In this paper [3], a highly secured vault is used to store the passwords. In this case, online vaults are at a risk of being attacked by hackers while offline vaults may leave several database copies across the devices which increases the risk of database compromise. Fake passwords can also be stored to make compromised passwords hard to use. In this paper [4], the system generates fake passwords which are similar to the correct one and encrypts and stores them along with the encrypted correct one. This makes it difficult for the attacker to guess. Since most websites provide limited attempts for login in case of invalid passwords the chance of compromise of the website account reduces further and the value of database decreases. A decentralized file is used to save the encrypted data in the local databases to avoid single point of failure [4].

Along with security there is also a need of availability. The passwords must be accessible across platforms and devices and be available at all times. In this paper [5], cloud services are used to provide access across devices and also allow synchronization between them. It also uses biometrics like fingerprint and face detection for better security. In this paper [6], a USB storage is used to store the user credentials. This reduces the chance of compromise on the server side or and even on the client side. The USB storage makes it simpler for the user to use it on different devices. Most password managers are of retrieval type. They retrieve the passwords from a local or remote database. The passwords are stored in encrypted form in these database. Though the problem with them is that online databases are very attractive for hackers as they can provide a comparatively very good value to them. On the other hand, offline database in the case where the password manager is accessed from many devices could leave database copies across all the devices and these could be compromised. Generative password manager is another type of password manager. Instead of storing passwords along with encryption and decryption to ensure its use and safety the generative password manager generates password on demand. In this paper [7], a generative password manager is used. It uses two keys for password generation. First is the user side part and second is the server part. This removes the single point of failure in case of a master password driven password manager. It also provides a web browser application which can be accessed anywhere using the master password [7]. The application also has some good retrieval features that have guaranteed results in the case of a security breach. Though still better usability is still required which may be incorporated by using biometrics or access control using the device's identity.

## III. PROPOSED SYSTEM

Taking into account the various positives of other similar systems as well as their points of failures, the proposed system will have the required as well as desired features to make it a much more advanced and robust than other current systems. To make it accessible across devices and platforms the system would have an android application for mobile devices and web browser extensions for PCs. So, the same account could be accessed at the same time on various devices. The system uses cloud computing to provide a secure and reliable environment. This also helps keep the data available at all times.

A user would have to provide his account id and a strong master password for his account. The system would use certain parameters to ensure the master password is strong i.e. it consists of different characters like numbers, special characters, etc. This will ensure that the master password, an important key to the user's password manager is not easy to crack. This master password is also used for generating complex passwords for user's accounts. OTP using SMS and

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

E-mail is used to provide 2 step verification. This will provide another level of protection. To further improve security, access control would be provided using MAC address of the user's registered devices. Use of GPS to check for unauthorized access can be done by analysing the location with respect to previous recent locations. The proposed application is a bilateral generative password manager i.e. it generates passwords for the user to use instead of retrieving them from the database. The critical point of a user using a weak password can be avoided by having the passwords generated by the application itself. So for a new website account the user will just have to log into the system and select that website account or create a new entry and input the website address and the account id. The application will then send a secret key from the user's device to the server and use it along with the server side key to generate a complex password. The user can then set this complex password as his new password. The generated passwords would be complex and also have high entropy. This will ensure strong as well as different passwords for all accounts. To improve usability of the application and also provide convenience, the application would autofill the user's website credentials whenever desired. This would help simplify the use of the proposed system in normal day-to-day browsing and would just require a login to access all accounts. A record of all recent activities related to the user's password modification would be kept to allow the user to keep track if any unauthorized activity takes place.

A recovery key is also provided to the user. In case of loss or compromise of master password, the recovery key would allow the user to regain access to his account and set a new master password. But the user would still need access to his mobile phone or his email id to complete the 2 step verification. This would ensure that the recovery tool is not used to gain backdoor entry into the user's account by an unauthorized person.

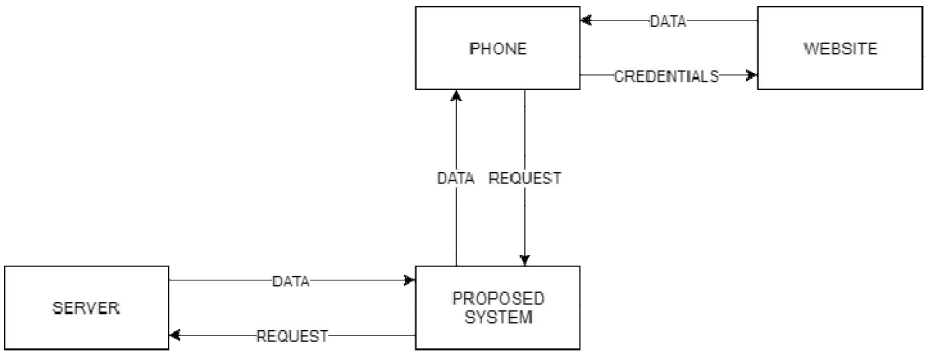


*Fig. 1 : Flow of Proposed System*

In case of compromise of the master password, the account can be recovered using the recovery key. If the server gets compromised, still it wouldn't compromise the user's account data as the secret key on the user's mobile phone is also needed to make sense of the data.

## IV. CONCLUSION

In this paper, the problems with regards to passwords are studied. A survey of alternate solutions has been done. The study of various related papers and some research about the problem related to passwords and password managers have led to a number of positive as well as vulnerable points. We have proposed a system that provides strong security while maintaining reasonable usability. It is a new secure architecture for password management that simplifies the authentication process from the user's side and avoids the single point of failure associated with congregating sensitive information in one location. Additionally, we created a strong password generation method which provides the users with extremely high entropy passwords without any associated burden.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

## V. FUTURE SCOPE

An application related to security cannot ever continue to exist in the same state. No system is impregnable or 100% secure. So, the proposed system needs to be robust and keep up to date to secure itself and its users against new challenges and attacks. Biometrics as a mode for authentication can be used instead of or along with the master password to further improve security and also the usability. User behavior analysis can also be incorporated later to identify the user using his/her pattern of use of device and the password manager. This system can also be further modified to work as a secure vault not only for passwords but also for important data in the form of text, media, etc. It can be used to provide restricted access to accounts, services, etc. Paid services can be provided with restricted access only to subscribed users. This can help reduce unauthorized access to paid services, information, etc.

## REFERENCES

[1] Yan, A. Blackwell, R. Anderson and A. Grant, "Password memorability and security: Empirical results," IEEE Security & Privacy Magazine, 2004.
[2] S. Istyaq and M. S. Umar, "Encoding Passwords using QR Image for Authentication," 2nd International Conference on Next Generation Computing Technologies, 14-16 October 2016.
[3] R. Chatterjee, J. Bonneau, A. Juels and T. Ristenpart, "Cracking resistant password vaults using natural language encoders," IEEE Security & Privacy, 2015.
[4] L. Wang, Y. Li and K. Sun, "Amnesia: A Bilateral Generative Password Manager," IEEE 36th International Conference on Distributed Computing Systems, 2016.
[5] A. S. Sodiya, A. T. Akinwale and J. Adeniran, "A Secured Mobile-Based Password Manager," International Conference on ICDIPC, 2016.
[6] X. Wang, Z. Han and D. Zhang, "IDKeeper: A Web Password Manager with Roaming Capability Based on USB Key," International Conference on Industrial Control and Electronics Engineering, 2012.
[7] B. Yang, H. Chu, G. Li, S. Petrovic and C. Busch, "Cloud Password Manager Using Privacy Preserved Biometrics," IEEE International Conference on Cloud Engineering, 2014.